

U.S. Department of Justice

Federal Bureau of Investigation

File No.

Office of the Legal Attache
1201 Roxas Boulevard, Ermita
Manila, Philippines
August 15, 2011

Director Magtanggol B. Gatdula
National Bureau of Investigation
Taft Avenue
Manila, Philippines
Attn: Atty
Chief, Foreign Liaison Division

b6
b7C

RE: To provide information regarding possible cyber attacks against law enforcement personnel

Dear Director Gatdula,

(U) The Federal Bureau of Investigation, US Embassy Manila, is providing the following information for your situational awareness regarding a current cyber threat targeting law enforcement personnel. Please forward this information to other NBI Divisions as appropriate.

(U//~~FOUO~~) (U) Law Enforcement at Risk for Harrassment and Identity Theft through "Doxing"

(U) ~~LAW ENFORCEMENT SENSITIVE~~: This information is the property of the Federal Bureau of Investigation (FBI) and may be distributed to federal, state, tribal, or local government law enforcement officials with a need-to-know. The information contained in this intelligence bulletin has been collected in support of an authorized law enforcement purpose of the FBI. Further distribution without FBI Headquarters authorization is prohibited. Precautions should be taken to ensure this information is stored or destroyed in a manner that precludes unauthorized access.

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

[REDACTED]

(U//~~FOUO~~) The FBI assesses with high confidence that law enforcement personnel and hacking victims are at risk for identity theft and harassment through a cyber technique called “doxing.” “Doxing” is a common practice among hackers in which a hacker will publicly release identifying information including full name, date of birth, address, and pictures typically retrieved from the social networking site profiles of a targeted individual.

(U//~~FOUO~~) In response to law enforcement activities that have occurred against Anonymous and LulzSec since January 2011, members of these groups have increased their interest in targeting law enforcement in retaliation for the arrests and searches conducted. Hackers and hacktivists—hackers who commit a computer crime for communicating a socially or politically motivated message—have been openly discussing these activities on an identified US social networking service and posting information pertaining to law enforcement on their accounts and Internet Relay Chat (IRC) channels.

- (U//~~FOUO~~) In June 2011 members of Anonymous and LulzSec discussed an identified US Government (USG) employee in the IRC channel #lulzsec. The detailed information included when he or she started working for the USG, training, assignments, and previous employment. FBI analysis suggests that this information was derived from a 2009 affidavit that was available on the Internet.
- (U//~~FOUO~~) On 26 July 2011, an identified US social networking service account used by members of Anonymous, warned of the intention to “dox” USG employees following the 19 July 2011 arrests of 16 individuals for their presumed role in Anonymous’ activities.
- (U) On 31 July 2011 more than 70 law enforcement Web sites were hacked and large amounts of confidential data was exfiltrated. These Web sites included state and local police departments that were not associated with the takedowns. The data consisted of e-mail addresses, usernames, Social Security numbers, home addresses, phone numbers, password dumps, internal training files, informant lists, jail inmate databases, and active warrant information. Operation AntiSecd claimed that the intrusion was in response to “bogus, trumped-up charges” against the individuals associated with Anonymous’ attacks on an identified US Internet money transfer service.

(U//~~FOUO~~) Recently, Anonymous members have also “doxed” the employees of companies that were victims of their previous attacks, who are perceived as working with law enforcement.

- (U) In July 2011 a sealed search warrant affidavit pertaining to the 19 July takedown was available on the Internet. The affidavit contained the personal information of employees of two US companies, as well as USG personnel. The personal information consisted of names,

units, and job titles.

(U) Outlook and Implications

(U//~~FOUO~~) The 19 July takedown of Anonymous and LulzSec members has increased members' interest in targeting law enforcement in retaliation for the arrests and searches conducted. As more arrests are made against suspected members of Anonymous and LulzSec, the FBI expects hacking activities and "doxing" that targets law enforcement and government interests will continue. This could compromise investigations and result in harassment and identity theft of the individuals named in the "dox."

(U//~~FOUO~~) Precautionary measures to mitigate potential harassment and identity theft risk to being "doxed" include:

- Safeguarding material containing personal information pertaining to officers and named victims;
- Changing passwords and do not reuse passwords for multiple accounts;
- Using strong passwords;
- Monitoring credit reports;
- Monitoring online personal information, including what others post about you on services such as social networking sites;
- Being careful when giving out contact information; and
- Being aware of social engineering tactics aimed at revealing sensitive information.

End notes:

(U) High confidence generally indicates that the FBI's judgments are based on high-quality information or that the nature of the issue makes it possible to render a solid judgment. Medium confidence generally means that the information is credibly sourced and plausible, but can be interpreted in various ways, or is not of sufficient quality or corroborated sufficiently to warrant a higher level of confidence. Low confidence generally means that the information's credibility or plausibility is questionable, the information is too fragmented or poorly corroborated to make solid analytic inferences, or that the FBI has significant concerns or problems with the sources.

(U) Anonymous is an international hacktivist group responsible for denial-of-service attacks, Web site defacements, and computer intrusions.

(U) LulzSec is a hacker group consisting of overlapping members of Anonymous and responsible for various computer intrusions.

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

[redacted]

Should you have any questions, please contact ALAT [redacted] at our office,
[redacted] and reference file number
[redacted] You may be assured of our continued cooperation in all matters of mutual
professional interest.

Sincerely,

[redacted]
Legal Attache

JDW:jdw

1 - Addressee

1 - [redacted]